PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-020782
(43)Date of publication of application : 23.01.1998

(51)Int.Cl. G09C 1/00
G06F 15/00
H04L 9/10

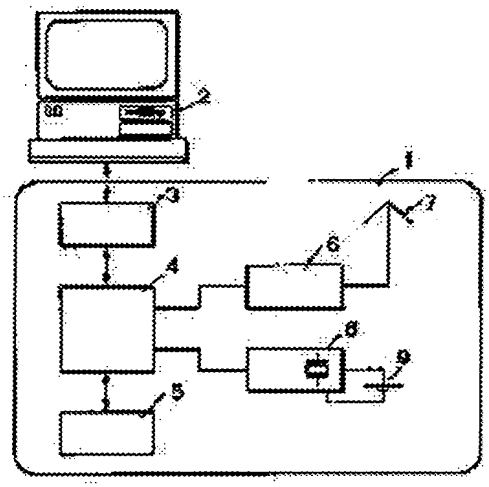
(21)Application number : 09-059708
(22)Date of filing : 14.03.1997

(71)Applicant : DEUTSCHE TELEKOM AG
(72)Inventor : HUBER KLAUS
TOENSING FRIEDRICH DR

(30)Priority
Priority number : 96 19610401 Priority date : 16.03.1996 Priority country : DE

(54) DETECTION METHOD AND DEVICE OF EXECUTION TIME OF ENCIPHERING PROCESS

(57)Abstract:
PROBLEM TO BE SOLVED: To document the execution of the improved enciphering process by using a taken time mark as a mark corresponding to the time information derived from a clock of which the adjustment is impossible.
SOLUTION: A document in a computer 2, is coded before the transmission by using a processer 4, and is signed in some cases. The transmission is performed through, for example, an interface of the computer 2 and a communication network. And the clocks 6, 7 for inserting the time marking, is scanned. The both time informations (data) are compared. The time information (data) of a radio clock 6 is added to the document as the time marking, when the time difference is less than a predetermined value, then is coded with the document continuously, and is signed in some cases. The time mark taken in this way, is the mark corresponding to the time information derived from the (unadjustable) clock 6 which can not be adjusted.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Japanese Patent Laid-open Publication No. HEI 10-20782 A

Publication date: January 23, 1998

Applicant: DEUTSCHE TELEKOM AG

Title: DETECTION METHOD AND DEVICE OF EXECUTION TIME OF ENCIPHERING PROCESS

[0015] According to a device structure of the present invention relating to a device for detecting the time that a transaction is executed, time information that is loaded (or inserted or contained), as a time mark, in a forgery- (or tamper- or illegality-) proof unit, in a document relating to the transaction is extracted from a clock that cannot be adjusted (an unadjustable clock). Furthermore, according to another device structure of the present invention, in a method for detecting the time that a document is created, signed, transmitted and/or received, a time mark loaded (or inserted or contained) in a document relating to a transaction in a forgery- (or tamper- or illegality-) proof unit, and the time mark corresponds to time information (data) that is extracted from a clock that cannot be adjusted (an unadjustable clock).

[0016] More advantageously, the clock, together with an autonomous current source, is arranged, so as to be inaccessible, except for time information calling, in a cryptomodule.

[0017] A cryptomodule with memories subjected to processes for protecting from outside modifications can be performed and implemented in various forms. In a preferred embodiment of the present invention, the cryptomodule is configured as a chip card.

[0018] According to a further embodiment of the present invention, the clock is provided as an accurate clock, for example, a quartz clock or a radio clock. To increase accuracy, a quartz clock, as well as an accurate clock, is provided in the cryptomodule.

[0024]

[Embodiments] According to the embodiment shown in the drawings, a cryptomodule 1 is connected to a computer 2 in which a document is created or processed. The cryptomodule has an interface 3 for connecting the computer 2 to a processor 4 in the cryptomodule 1. Filed in a memory 5 are algorithms and constants for coding, creating electronic signatures, and generating time markings (to be inserted into documents).

[0025] The processor 4 is further connected to a radio clock 6. The radio clock receives, via an antenna 7, signals from a time code transmitter. A quartz clock 8 is connected to the processor 4 and always maintained its operational state by a battery 9.

[0026] A document that is created in a well-known format in the computer 2 is coded prior to being sent by using the processor 4,

and signed in some cases. The document can be sent through, for example, an interface (not shown) of the computer 2 and a communication network. According to the shown embodiment, the clocks 6 and 8 are scanned in order to insert time markings. Time information (data) of the clock 6 is compared to that of the clock 8. If the time difference therebetween is smaller than a predetermined value, the time information (data) of the radio clock 6 is added, as a time marking, to the document, subsequently coded together with the document and, in some cases, a signature is attached to the document.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－20782

(43)公開日　平成10年(1998)１月23日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ　1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６４０Ｚ	
Ｇ０６Ｆ　15/00	３３０		Ｇ０６Ｆ　15/00	３３０Ａ	
Ｈ０４Ｌ　9/10			Ｈ０４Ｌ　9/00	６２１Ｚ	

審査請求　未請求　請求項の数18　ＯＬ　（全５頁）

(21)出願番号　特願平9－59708

(22)出願日　平成９年(1997)３月14日

(31)優先権主張番号　１９６１０４０１．７

(32)優先日　1996年３月16日

(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　595135947
ドイチェ　テレコム　アクチエンゲゼルシャフト
ドイツ連邦共和国　ボン　ゴーデスベルガー　アレー　87091

(72)発明者　クラウス　フーバー
ドイツ連邦共和国　ダルムシュタット　エルンストールートヴィッヒーシュトラーセ　21

(72)発明者　フリードリッヒ　テンズィング
ドイツ連邦共和国　ヘキスト　ツム　ハルトベルク　15

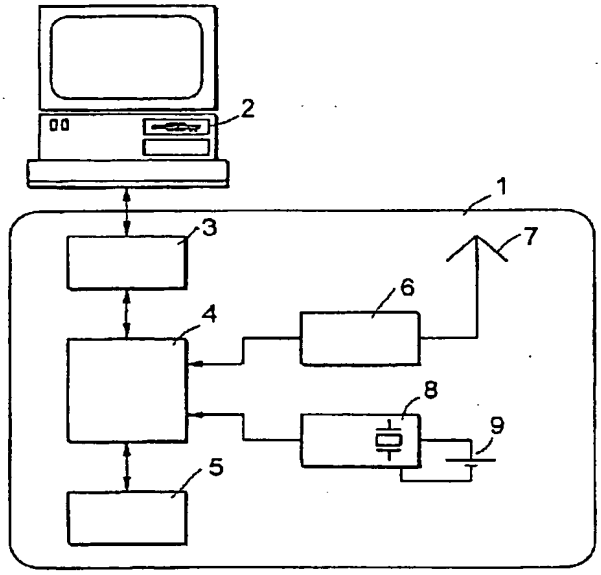
(74)代理人　弁理士　矢野　敏雄　（外３名）

(54)【発明の名称】　暗号化処理プロセスの実行時点の検出方法及び装置

(57)【要約】

【目的】　暗号化処理プロセスの実行、実施又はトランザクション（処理、取引）の実行、実施をドキュメント化（文書化）し得る方法及び装置を提供すること。

【構成】　トランザクションの実行時点又はドキュメントの作成、署名、送信及び及び／又は受信の時点の検出方法において、時間マークをドキュメント内に偽造（ないし改ざん又は不正）防止手段を施して取り込み（挿入ないし収録し）、前記時間マークは、調整操作の不可能な（調整不能の）時計からひき出される時間情報（データ）に相応するものであるようにしたこと。



1

【特許請求の範囲】

【請求項１】　トランザクションの実行時点の検出方法において、

時間マークをトランザクションに係わるドキュメント内に偽造ないし改ざんされないように（偽造ないし改ざん又は不正防止手段を施して）取り込み（挿入ないし収録し）、前記時間マークは、調整操作の不可能な（調整不能の）時計からひき出される時間情報（データ）に相応するものであるようにしたことを特徴とする暗号化処理プロセスの実行時点の検出方法。

【請求項２】　ドキュメントの作成、署名、送信及び及び／又は受信の時点の検出方法において、

時間マークをトランザクションに係わるドキュメント内に偽造（ないし改ざん又は不正）防止手段を施して取り込み（挿入ないし収録し）、前記時間マークは、調整操作の不可能な（調整不能の）時計からひき出される時間情報（データ）に相応するものであるようにしたことを特徴とする暗号化処理プロセスの実行時点の検出方法。

【請求項３】　当該時計は、歩度の精確な時計、例えば、水晶時計であるようにしたことを特徴とする請求項１又は２記載の方法。

【請求項４】　前記時計は無線時計であるようにしたことを特徴とする請求項１又は２記載の方法。

【請求項５】　更なる時間情報（データ）を歩度の精確な時計、例えば、水晶時計から取出すようにし、そして、両時計時間マークは、相互に比較され、そして、所定の時間差より大の時間差の場合、時間マークの発生が行われず、及び／又は誤りのメッセージ（通報）が出力されるようにしたことを特徴とする請求項４記載の方法。

【請求項６】　所定の時間差より小さい時間差の場合、無線時計の時間情報を時間マークのために使用することを特徴とする請求項５記載の方法。

【請求項７】　付加的に場所位置マーキングをドキュメント内に取り込み（挿入ないし収録し）、前記の両場所位置マーキングは、位置測定系により生ぜしめられるようにしたことを特徴とする請求項１から６までのうちいずれか１項記載の方法。

【請求項８】　時間マーク及び場合により場所位置マーキングを、少なくとも１つの遠隔のところに配置されている装置により暗号手法的な不正防止手段を施して伝送するようにしたことを特徴とする請求項１から７までのうちいずれか１項記載の方法。

【請求項９】　トランザクションの実行の時点検出のための装置において、

時間マークとして偽造（ないし改ざん又は不正）防止手段を施してトランザクションに係わるドキュメント内に取り込まれる（挿入ないし収録される）時間情報が、調整操作の不可能な(調整不能の)時計（６、８）から引き出されるように構成されていることを特徴とする暗号化処理プロセスの実行時点の検出装置。

2

【請求項１０】　ドキュメントの作成、署名、送信及び及び／又は受信の時点の検出装置において、

時間マークが、トランザクションに係わるドキュメント内に偽造（ないし改ざん又は不正）防止手段を施して取り込まれ（挿入ないし収録され）、前記時間マークは、調整操作の不可能な（調整不能の）時計（６、８）からひき出される時間情報（データ）に相応するものであるように構成されていることを特徴とする暗号化処理プロセスの実行時点の検出装置。

【請求項１１】　前記時計（８）は、自律的電流源と共に、時間情報の呼出のため以外にはアクセス不能に暗号化モジュール（１）内に配置されていることを特徴とする請求項９又は１０記載の装置。

【請求項１２】　前記暗号モジュール（１）は、チップカードとして構成されていることを特徴とする請求項１１項記載の装置。

【請求項１３】　前記時計は、歩度の精確な時計、例えば水晶時計（８）であることを特徴とする請求項１から９までのうちいずれか１項記載の装置。

【請求項１４】　前記時計は、無線時計（６）であることを特徴とする請求項９から１２までのうちいずれか１項記載の装置。

【請求項１５】　更なる時間情報（データ）は、歩度の精確な時計、例えば水晶時計から引き出し可能であり、両時間情報（データ）は、相互に比較され、そして、所定の時間差より大の時間差の場合、時間マーキングが発生されず、及び／又は、誤りメッセージ（通報）が出力されるように構成されていることを特徴とする請求項１４記載の装置。

【請求項１６】　所定の時間差より小の時間差の場合、時間マーキングに対する無線時計（６）の時間情報（データ）が使用されることを特徴とする請求項１５記載の装置。

【請求項１７】　暗号化モジュール内に位置測定装置、例えば、ＧＰＳ受信機が設けられており、該受信機からは、ドキュメント中に取り込まれるべき（挿入ないし収録さるべき）位置マーキングの形成のためそれぞれの位置情報（データ）が引き出し可能でることを特徴とする請求項９から１６までのうちいずれか１項記載の装置。

【請求項１８】　時間情報（データ）及び場合により位置マーキングが、少なくとも１つの遠隔配置された装置により暗号化手法で保護を施されて送信されるように構成されていることを特徴とする請求項９から１７までのうちいずれか１項記載の装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化処理プロセスの実行時点の検出方法並びに装置に関する、即ち、トランザクションの実行時点の検出方法及びドキュメント

3

の作成、署名、送信及び及び／又は受信の時点の検出方法に関する。

【０００２】

【従来の技術】通信技術の最新の手法、例えばデジタルないし電子的署名により、ドキュメントの認証及び完全性を種々のフォーム（形態）で確保することが可能になる。関連する手法は、例えば、Ｗ．Ｆｕｍｙ、Ｈ．ＰＲｉｅβの著書：Ｋｒｙｐｔｏｇｒａｐｈｉｅ、２．Ａｕｆｌａｇｅ（第二版）、Ｏｌｄｅｎｂｏｕｒｇ Ｖｅｒｌａｇ（出版社）、１９９４に記載されている。そのようにして、ドキュメントを偽造ないし改ざんから保護することが可能である。電子的著書を生成する現在慣用の手法は、屡々チップカードを使用し、該チップカード中には不当な読み取りの防止のための秘密な鍵及び暗号化プロセッサが設けられている。普及している手法は、所謂ＲＳＡ－手法であり、該手法は、下記刊行物に記載されている。

【０００３】Ｒ．Ｌ Ｒｉｖｅｓｔ、Ａ．Ｓｈａｍｉｒ、Ｌ．Ａｄｌｅｍａｎ：Ａ Ｍｅｔｈｏｄ ｆｏｒ Ｏｂｔａｉｎｉｎｇ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅｓａｎｄ Ｐｕｂｌｉｃ Ｋｅｙ Ｃｒｙｐｔｏｓｙｓｔｅｍｓ、Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ ｏｆ ｔｈｅ ＡＣＭ、Ｖｏｌ．２１ Ｎｏ．２、ｐｐ．１２０－１２６、Ｆｅｂ．１９７８。

【０００４】屡々、法律上重要な内容を有するドキュメント（文書）の場合、例えばトランザクション（取引、処理）又は委託業務ないし代理契約（例えば有価証券取引における）に係わるドキュメントの場合、ドキュメントの作成、署名、又は送付の時点が重要である。

【０００５】

【発明が解決すべき課題】本発明の課題とするところは、改善（改良）された暗号化処理プロセスの実行、実施の時点の検出方法及び装置、即ち、例えば、ドキュメントの電子的署名、ドキュメントの作成、送付または受信又はトランザクション（処理、取引）の実行、実施を、偽造ないし改ざんされないように（偽造防止手段を施して）ドキュメント化（文書化）し得る方法及び装置を提供することにある。ここで、ドキュメントを作成する、又は署名する人物も当該の実行、実施時点を偽造ないし改ざんし得ないようにするものである。

【０００６】

【課題を解決するための手段】上記課題の解決のため、本発明によれば、トランザクションの実行時点の検出方法において、時間マークをトランザクションに係わるドキュメント内に偽造ないし改ざんされないように（偽造ないし改ざん又は不正防止手段を施して）取り込み（挿入ないし収録し）、前記時間マークは、調整操作の不可能な（調整不能の）時計からひき出される時間情報（データ）に相応するものであるようにしたのである。

【０００７】亦、上記課題は、本発明のさらなる方法によれば、ドキュメントの作成、署名、送信及び及び／又は受信の時点の検出方法において、次のようにして解決される。即ち、時間マークをトランザクションに係わるドキュメント内に偽造（ないし改ざん又は不正）防止手段を施して取り込み（挿入ないし収録し）、前記時間マークは、調整操作の不可能な（調整不能の）時計からひき出される時間情報（データ）に相応するものであるようにしたのである。

4

【０００８】本発明の方法は、次のようなすべてのドキュメントにおいて適用され得る、即ち、データの形態で存在するものであって、作成され、署名され、又は他の仕方で処理されるすべてのドキュメントにおいて適用され得る。ドキュメント中へ時間マーキングを偽造ないし改ざんの防止されるように収録する（取り込む）ことにより、一度適正に施された（為なされた）時間マーキングの事後的な偽造ないし改ざんが回避される。本発明の方法の適用例は、自動キャッシング機における現金引き出しのようなトランザクション及び電話ー通話のなされた時点の検出である。

【０００９】時間マーキングは、本発明の方法では、日付け情報（データ）、通常の形態（年、月、日、時間）での日付けー及び時計時間情報（データ）から成り、又は、コード化形態で生ぜしめられ得、例えば、時計のカウント値として生ぜしめられ得、上記時計は、所定の時点を起点としてたんに、水晶発振器のクロック周期をカウントする（上記クロック周期を通常の時間単位にコード化することなく）。

【００１０】調整操作の不可能な（調整不能の）時計としては、本発明の方法では歩度の精確な時計、例えば水晶時計又は、無線時計が使用される。後者は、長期的にも高い歩度ー精度が確保され、又電池の交換後再び適正な時間情報（データ）が調整セッティングされるという利点を有するが、外部から、相応の技術手段の適用の下で操作影響を受け、以て、偽造ないし改ざんされ得るおそれがある。

【００１１】このことを回避するため、本発明の方法の発展形態によれば、更なる時間情報（データ）が歩度の精確な時計、例えば、水晶時計から取出されるようにし、そして、両時計時間マークは相互に比較され、そして、所定の時間差より大の時間差の場合、時間マークの発生が行われず、及び／又は誤りのメッセージ（通報）が出力されるようにしたのである。有利には、所定の時間差より小さい時間差の場合、無線時計の時間情報を時間マークのために使用するのである。

【００１２】時間差は、次のように選定するとよい、即ち、水晶時計の所与の精度のもとで当該の時間差は、想定さるべき動作時間内で所定の時間差より大でないように選定するとよい。但し、所定の時間差は、次のような大きさのオーダにすべきである、即ち、当該の時点の検出上クリティカルでないような大きさのオーダにすべき

5

である。そのようにすれば、時間差が所定値を下回る場合に無線時計の時間情報（データ）の偏差があっても不都合なことは起こらない。但し、偽造ないし改ざんの場合一層大きな時間差が起こると時間マーキングの作成はもはや可能でない。場合により適当な誤り（エラー）メッセージ（通報）が、例えば、当該の状態を表すプロトコル（取り込み（挿入ないし収録））のプリントアウトにより行われ得る。

【００１３】本発明の発展形態によれば、付加的に場所位置マーキングをドキュメント内に取り込み（挿入ないし収録）し前記の両場所位置マーキングは、位置測定システムにより生ぜしめられるようにしたのである。

【００１４】調整操作の不可能な（調整不能の）時計及び場合により位置測定装置は、本発明の更なる発展形態によれば次のようにして実現することもできる、即ち、時間マーク及び場合により場所位置マーキングを、少なくとも１つの遠隔のところに配置されている装置により暗号手法的な不正防止手段を施されて伝送されるようにしたのである。

【００１５】トランザクションの実行時点検出装置に係わる本発明の装置構成によれば、トランザクションの実行の時点検出のための装置において、時間マークとして偽造（ないし改ざん又は不正）防止手段を施してトランザクションに係わるドキュメント内に取り込まれる（挿入ないし収録される）時間情報が、調整操作の不可能な（調整不能の）時計から引き出されるように構成されているのである。さらに、本発明の別の装置構成によれば、ドキュメントの作成、署名、送信及び及び／又は受信の時点の検出方法において、時間マークをトランザクションに係わるドキュメント内に偽造（ないし改ざんないし不正）防止手段を施して取り込み（挿入ないし収録し）、前記時間マークは、調整操作の不可能な（調整不能の）時計からひき出される時間情報（データ）に相応するものであるようにしたのである。

【００１６】更に有利には、前記時計は、自律的電流源と共に、時間情報の呼出のため以外にはアクセス不能に暗号化モジュール内に配置されているのである。

【００１７】外部からの変更に対する防止手段を施されているメモリをを有する暗号化モジュールを種々の形態で実行、実施し得る。本発明の有利な実施形態では、前記暗号モジュールは、チップカードとして構成されているのである。

【００１８】更に本発明の実施形態によれば、前記時計は、歩度の精確な時計、例えば水晶時計であり、又は、無線時計として構成さているのである。確実性の向上のため、歩度の精確な時計のみならず水晶時計をも暗号化モジュール内に設け得る。

【００１９】時間マーキングの偽造ないし改ざんの防止能力の向上のため本発明の装置構成によれば、更なる時間情報（データ）は、歩度の精確な時計、例えば水晶時

6

計から引き出し可能であり、両時間情報（データ）は、相互に比較され、そして、所定の時間差より大の時間差の場合、時間マーキングが発生されず、及び／又は、誤りメッセージ（通報）が出力されるように構成されているのである。

【００２０】有利には、所定の時間差より小の時間差の場合、時間マーキングに対する無線計算の時間情報（データ）が使用されるのである。

【００２１】本発明の装置の発展形態によれば、暗号化モジュール内に位置測定装置、例えば、ＧＰＳ受信機が設けられており、該受信機からは、ドキュメント中に取り込み（挿入ないし収録）さるべき位置マーキングの形成のためそれぞれの位置情報（データ）が引き出し可能であるように構成されているのである。

【００２２】調整不能時計及び場合により、位置測定装置は、本発明によれば、次のようにして、実現することもできる、即ち、時間情報（データ）及び場合により位置マーキングが、少なくとも１つの遠隔配置された装置により暗号化手法で保護を施されて伝送されるように構成されているのである。

【００２３】本発明の１実施例が図示してあり、以下詳述する。

【００２４】

【実施例】図示の実施例では、暗号化モジュール１は、コンピュータ２に接続されており、該コンピュータ中では、ドキュメント（文書）が作成され、又は処理される。暗号化モジュールは、コンピュータ２を暗号化モジュール1のプロセッサ４と接続するためのインターフェース３を有する。メモリ５内にはコード化のため、電子署名の形成のため及び時間マーキング（これはドキュメント内に挿入される）の生成のためアルゴリズム及び定数がファイルされている。

【００２５】更に、プロセッサ４は。無線時計６と接続されており、該無線時計は、アンテナ７を介して時間符号送信機の信号を受信する。更に、プロセッサ４にて水晶時計８が接続されており、該水晶時計は、電池９により常時に作動状態に保持される。

【００２６】それ自体公知の型式で、コンピュータ２内で作なされたドキュメントが、プロセッサ４を用いて送信前にコード化され、場合により署名される。送信は、例えばコンピュータ２の図示していないインターフェース及び通信ネットワークを介して行われ得る。図示の実施例では時間マーキングの挿入のため時計６、８がスキャニングされる。両時間情報（データ）が比較される。時間差が所定値より小である場合、無線時計６の時間情報（データ）が、時間マーキングとしてドキュメントに追加され、それに引き続いて、ドキュメントと共にコード化され、そして、場合により署名される。

【００２７】

【発明の効果】本発明によれば、改善（改良）された暗

7　　8

号化処理プロセスの実行、実施の時点の検出方法及び装置、即ち、暗号化処理プロセスの実行、実施の時点、例えば、ドキュメントの電子的署名、ドキュメントの作成、送付または受信又はトランザクション（処理、取引）の実行、実施をドキュメント化（文書化）し得る方法及び装置を実現し得、ここで、ドキュメントを作成する、又は署名する人物も当該の実行、実施時点を偽造ないし改ざんし得ないようにすることができるという効果が奏される。

【図面の簡単な説明】

【図１】本発明の方法を実施した装置の実施例のブロック接続図である

【符号の説明】

1	暗号化モジュール
2	コンピュータ
3	インターフェース
4	プロセッサ
5	メモリ
6	無線時計
7	アンテナ
8	水晶時計
9	電池

【図１】